ABSTRACT

A method and system for performing on behalf of a registered user an operation on data stored on a publicly accessible data access server coupled to a client machine used by the registered user in such a manner as to prevent unauthorized users from using the data and without requiring decryption by the client machine. The registered user has a unique identifier known to the data access server and further having a password accessible to the data access server. The unique identifier is saved in the data access server in a user space associated with the registered user, who further has a public key and a private key that is encrypted with the password to generate an encrypted private key that is stored together with the public key in the user space. The data access server receives from a user a login request including an identifier of the user and supplementary data that may be used to authenticate the user. It receives a request by a registered user for performing an operation together with a session ID of the user that is allocated to the user during login and is known to a login server connected to the data access server and to which it communicates the session ID for identification thereby, and for receiving from the login server the user's password encrypted in such a manner as to enable decryption by the data access server. The encrypted password is decrypted so as to derive the password associated with the user during the login request, thus enabling the data access server to decrypt the encrypted private key of the registered user and use the registered user's private key to perform the requested operation.